REMARKS

Claims 1-3, 5, 6, 8-10, 41, 42, 44, 45, and 47-56 are currently pending. Claim 1 has been slightly amended to correct for an ambiguous typographical error. It is respectfully submitted that no new matter has been added.

Claim Rejections under 35 U.S.C. 102(e)

Applicant has amended the claims to advance prosecution and does not explicitly or implicitly admit a need for amendment of the claims.

The Patent Office rejected claims 1, 3, 5, 6, 8-10, 42, 44, 45, 47-50, and 52-56 under 35 U.S.C. 102(a) as being anticipated by Fruehauf, U.S. Patent No. 7,149,308.

Although the claims stand on their own, for the purposes of certain aspects of the claimed invention, claim 1 will now be discussed.

The embodiments described in Applicant's specification allow a STB to be configured to receive messages addressed to it. Configuration comprises sending message detection data including an address and a corresponding key, all encrypted with a key specific to the STB, decrypting this at the STB using the unique key, storing the address and the corresponding key, and subsequently using the stored address (i.e. the address that was broadcast by the network) to identify messages addressed to the STB that are derived from a different network, these messages being decrypted by the key corresponding to the address and received over the broadcast network.

The embodiments allow the STB to be configured with an address remotely, i.e. after sale, and without requiring access to a bidirectional network, so that messages sent to that address can be detected by the STB. In the prior art, conversely, no such remote configuration with an address is disclosed. The embodiments allow broadcast of an addressed message that is decipherable only by the STB that is configured to receive messages with that address.

None of the prior art of record discloses "sending to a digital broadcast receiver through a digital broadcast network message detection data ... comprising: a) at least one individual address corresponding to said digital broadcast receiver, ... storing said ... at least one individual address ... in said digital broadcast receiver [and] using the stored individual address to identify that [a] message sent through said digital broadcast network is addressed to said digital broadcast receiver". Furthermore, Applicant contend that it would not be obvious to modify the prior art in such a way as to provide this combination of features.

Additionally none of the prior art of record discloses encrypting a broadcast message using a key that is specific to a digital broadcast receiver. Claim 1 recites "sending to a digital broadcast receiver through a digital broadcast network message detection data ... comprising: a) at least one individual address corresponding to said digital broadcast receiver, wherein said message detection data is encrypted using a key associated substantially uniquely with said digital broadcast receiver; decrypting said message detection data with said key associated substantially uniquely with said digital broadcast receiver at said digital broadcast; storing said decrypted message detection data, including the at least one individual address and the associated key, in said digital broadcast receiver so as to configure said digital broadcast receiver to detect messages individually addressed thereto and received through said digital broadcast network". By encrypting the message detection data with a key specific to the digital broadcast receiver, claim 1 allows the digital broadcast receiver to be configured to receive messages that are unable to be received by any other receivers.

Fruehauf discloses a system for cryptographic communication among multiple users and a central service provider, and describes this in relation to a cable television system. Fruehauf concentrates primarily on the use of seeds and in situ key generators, so as to reduce the burden of key generation and delivery that are said to be a problem with the prior art. The summary of the invention at column 2, line 48 to column 5, line 67 is useful in understanding the disclosure of Fruehauf.

Fruehauf discloses the configuration of a set-top box or cable modem 101. The most relevant passages are at page 7 line 57 to page 8 line 55. Here it can be seen that the set-top box 101 is given a temporary set-up seed, denoted as "X", by the installer.

From column 7 line 62 Fruehauf says that "Upon setup, the set top box or cable modem contacts Master Station 107 of the service provider, which has stored within its secure memory the same set-up seed "X" and can therefore decipher the incoming communication from the activated set top box or cable modem 101. After a secure channel is established using the set-up seed 210, the Master Station 107 then sends to the set top box or cable modem 101 a new, permanent, user unique individual seed "a" 211, which is decrypted in the set-top box or cable modem 101 and then stored in a secure memory 212. The Master Station 107 then stores the same seed "a" just transmitted in its secure memory 209 and links it to the new user's address/identification function assigned earlier. Once this operation is complete, the temporary set-up seed "X" in the user's set-top box or cable modem 101 is preferably deleted."

To summarise, Fruehauf uses a temporary seed "X" to o generate a key with which to encrypt communications with a Master Station 107 and to obtain therefrom a user unique individual seed "a", which is encrypted during communication by a key generated using the set-up seed "X".

There are two questions that need to be considered. The first is whether the seed "a" is a key that is used to encrypt data and that may be used to decrypt the encrypted data. It seems clear that the answer to this question is "no". Fruehauf is clear in its disclosure that seeds are used by a pseudo-random key generator system (PKG) for generating keys – see column 6 lines 38 to 51 of Fruehauf. However, the seeds are not, themselves, keys. The seeds are not used to encrypt or decrypt, so cannot be 'keys' according to the normal meaning of the term. The second is whether the seed constitutes an address, by which messages can be identified as being addressed to a particular receiver. We contend that the seed cannot be considered properly to constitute an address since, although the seed may be (quasi-)unique to a set-top box, Fruehauf does not disclose that a seed is used as an address.

Even if a seed could be considered to be an address corresponding to a digital broadcast receiver or an associated key (which is not conceded) it seems clear that a seed could not be considered to be both an address and an associated key simultaneously.

Properly construing claim 1 and properly understanding Fruehauf leads to an understanding that Fruehauf does not disclosure the features of claim 1 "sending to a digital broadcast receiver... message detection data comprising: a) **at least one individual address corresponding to said digital broadcast receiver**, and b) **for each individual address at least one associated key**" (emphasis added). Even if it were considered that the seed of Fruehauf constitutes one of these components of the message detection data (which is not conceded), it is clear that Fruehauf does not disclose both of these components.

Furthermore, stemming from the fact that Fruehauf does not disclose addressing set top boxes, otherwise perhaps through encrypted communications with a key generated from a seed specific to the set-top box, Fruehauf does not disclose the following features of claim 1 "sending a message...to said digital broadcast receiver...said message comprising: a) said **at least one individual address** and b) **message contents encrypted with** one of said at least **one associated key**" (emphasis added), neither does Fruehauf disclose "said digital broadcast receiver using the stored individual address to identify that said message sent through said digital broadcast network is addressed to said digital broadcast receiver; and decrypting said message at said digital broadcast receiver using said stored at least one associated key". To re-iterate, Fruehauf would seem to disclose using a key for decrypting, but does not disclose the use of an address and a key in the manner claimed in claim 1. Claim 1 is further distinguished from Fruehauf in that in claim 1 a key that is used to encrypt a message is transmitted as part of message detection data. In Fruehauf only a seed that is transmitted, and the seed is used by the set-top box to generate a key that is then used to decrypt a transmitted message – no message is encrypted with the seed.

As a consequence of the above, we contend that claim 1 is not anticipated by Fruehauf. Apparatus claim 10 is not anticipated by Fruehauf for similar reasons. In particular, claim 10 requires "a receiver configured to receive message detection data... comprising: a) at least one individual address corresponding to said digital broadcast receiver, [and] b) for each individual address, at least one associated key" and "said digital broadcast receiver configured to receive a message... comprising: a) said at least one individual address; and b) message content encrypted with one of said at least one associated key, said digital broadcast receiver being configured to use the stored at least one individual address to identify that the message received through said digital broadcast network is addressed to said digital broadcast receiver; and said digital broadcast receiver being configured to decrypt said message using said at least one associated key".

Method claim 50 corresponds closely to apparatus claim 10 and is contended not to be anticipated by Fruehauf for reasons corresponding to those given in relation to claim 10.

Claim Rejections under 35 U.S.C. 103(a)

The Patent Office rejected claims 2, 41, and 51 under 35 U.S.C. 103(a) as being unpatentable over Fruehauf in view of Thornton, U.S. Published Patent Application No. 2003/0056220.

As discussed above, Fruehauf does not disclosure the features of claim 1 "sending to a digital broadcast receiver... message detection data comprising: a) **at least one individual address corresponding to said digital broadcast receiver**, and b) **for each individual address at least one associated key**."

Thornton (U.S. published patent application no. 2003/0056220) concerns enabling users with independent terminal devices to share audiovisual content in the context of a communication session, shared software application, or common experience – see paragraph [0002].

Thornton is not seen to remedy the above noted deficiency of Fruehauf.

At least because neither Fruehauf nor Thornton discloses "sending to a digital broadcast receiver... message detection data comprising: a) **at least one individual address corresponding to said digital broadcast receiver**, and b) **for each individual address at least one associated key**," no purported combination of Fruehauf and Thornton would not make obvious any of claims 2, 41, and 51.

The Patent Office is respectfully requested to reconsider and remove the rejections of claims 1-3, 5, 6, 8-10, 41, 42, 44, 45, and 47-56 under 35 U.S.C. 102(e) based on Fruehauf and under 35 U.S.C. 103(a) based on Fruehauf in view of Thornton, and to allow all of the pending claims 1-3, 5, 6, 8-10, 41, 42, 44, 45, and 47-56 as now presented for examination. An early notification of the allowability of claims 1-3, 5, 6, 8-10, 41, 42, 44, 45, and 47-56 is earnestly solicited.

Serial No.: 10/535,062
Art Unit: 2617

Respectfully submitted:

Walter J. Malinowski October 23, 2009

Walter J. Malinowski Date

Reg. No.: 43,423

Customer No.: 29683

HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203) 925-9400, extension 19
Facsimile: (203) 944-0245
email: wmalinowski@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

10·23·2009 Jessica [illegible]

Date Name of Person Making Deposit